Listing of Claims:

1. (Currently Amended) A method for creating a computer identifier for an online customer for detecting a possible fraudulent transaction in the course of an online transaction comprising the steps of:

receiving, from [[said]] a customer's computer, at least one ~~personal or~~ non-personal identification parameter;

capturing, from [[the]] a clock of said customer's computer, said customer's computer local time;

capturing, from a clock of a website[['s]] server [[clock]], said website server's local
time;

creating and storing a delta of time parameter based upon the difference between said customer's computer local time and said website server's local time; and

~~uniquely~~ identifying said customer with said delta of time parameter and [[said]] at least one ~~personal or~~ non-personal identification parameter.

2. (Currently Amended) The method of Claim 1 further including the step of receiving, from said customer's computer, an additional identification parameter comprising personal identification information relating to said transaction.

3. (Currently Amended) The method of Claim 1 wherein said at least one non-personal identification parameter is said customer's computer's IP address.

4. (Currently Amended) The method of Claim 1 wherein said at least one non-personal identification parameter is said customer's computer's Browser ID.

5. (Original) The method of claim 1 wherein said delta of time parameter is stored as a range of time.

6.   (Original) A method for detecting fraud in an online transaction by a customer comprising the steps of:

        creating a first computer identifier in the course of an online transaction comprising the steps of Claim 1;

        creating at least a second computer identifier in the course of a second proposed online transaction comprising the steps of Claim 1;

        utilizing a matching parameter to compare said first computer identifier with said second computer identifier;

        creating a matching value based on the similarities between said first computer identifier and said second computer identifier; and

        classifying said second online transaction as fraudulent, not fraudulent, or requiring further consideration based upon the value of said matching parameter.

7.   (Currently Amended) The method in Claim 6, further comprising:

        communicating to [[the]] a website operator an indication, as to whether said second online transaction is fraudulent, not fraudulent, or requires further consideration.

8.   (Original) The method in Claim 6, further comprising:

        blocking said second online transaction based upon the value of said matching parameter.

9.   (Original) The method in Claim 6, further comprising:

        communicating to said customer the status of said second online transaction based upon the value of said matching parameter.

10.   (Original) The method in Claim 6, wherein said delta of time parameter is stated as a range of time.

11.   (Currently Amended) The method of claim 6 wherein said personal or non-personal identification parameter is a Browser ID.

12.   (Currently Amended) A computer readable medium containing program instructions for
creating a computer identifier in the course of an online transaction comprising ~~the steps of~~:

        ~~receiving,~~ computer code that receives from an online customer's computer, at least one
of either a personal or non-personal identification parameter;

        ~~capturing,~~ computer code that captures from [[the]] a clock of said customer's computer,
said customer's computer's local time;

        ~~capturing,~~ computer code that captures from [[the]] a clock of [[said]] a website[['s]]
server ~~computer~~, said website server ~~computer~~'s local time;

        ~~creating and storing~~ computer code that creates and stores a delta of time parameter based
upon the difference between said customer's computer's local time and said website server
~~computer~~'s local time; and

        ~~uniquely identifying~~ computer code that identifies said customer with ~~customer
identification~~ customer identification data that is based upon both ~~comprising~~ said delta of time
parameter and [[said]] at least one of either of said personal or non-personal identification
parameter.

13.   (Currently Amended) The computer readable medium of Claim 12 further including ~~the
step of~~:

        ~~receiving and storing,~~ computer code that receives and stores, from said customer's
computer, personal identification information relating to said transaction.

14.   (Currently Amended) The computer readable medium of Claim 12 further including ~~the
step of~~:

        ~~communicating~~ computer code that communicates to [[the]] a website operator an
indication as to whether a second online transaction ~~may be~~ is or is not fraudulent because of the
similarity existing between the stored customer identification data and [[the]] new customer[['s]]
identification data.[[.]]

15.   (Currently Amended) The computer readable medium of Claim 14 further including ~~the step of~~:

    ~~blocking~~ computer code that blocks said second online transaction based upon said indication as to whether a second online transaction ~~may be~~ is or is not fraudulent.

16.   (Currently Amended) The computer readable medium of Claim 14 further including ~~the step of~~:

    ~~communicating~~ computer code that communicates to [[said]] a customer the status of said second online transaction based upon the similarity of said stored customer identification data and the new customer[['s]] identification data.

17.   (Currently Amended) A computer readable medium as ~~claims~~ in claim [[11]]12 wherein said non-personal computer identification parameter is a Browser ID.

18.   (Currently Amended) A computer readable medium containing program instructions for detecting likelihood of fraud in an online transaction comprising ~~the steps of~~:

    ~~creating~~ computer code that creates a first computer identifier in the course of an online transaction comprising the steps of Claim 1;

    ~~creating~~ computer code that creates at least one additional computer identifier in the course of an additional online transaction comprising the steps of Claim 1;

    ~~utilizing~~ computer code that utilizes a matching routine to compare said first computer identifier with said at least one additional computer identifier; and

    ~~deciding~~ computer code that decides as to whether the online transaction is fraudulent, not fraudulent or requires further consideration based on the similarities between said first computer identifier and said at least one additional computer identifier.

19.   (New) A method for detecting a possible fraudulent online transaction comprising the steps of:

    receiving information relating to an online transaction from a customer's device;

capturing a local time from a clock of said customer's device;

capturing a website server's local time from a clock of a website server relating to said online transaction;

calculating a measured delta of time parameter based upon a difference between said customer's device local time and said website server's local time; and

comparing said measured delta of time parameter with a previously determined delta of time parameter associated with said customer's device for discrepancies indicating potential fraud.

20.   (New) The method of Claim 19 wherein said previously determined delta of time parameter was calculated from a previous online transaction between said customer's device and said website server.

21.   (New) The method of Claim 19 wherein said measured delta of time parameter is compared to said previously determined delta of time parameter to determine whether they are substantially the same.

22.   (New) The method of Claim 19 wherein said measured delta of time parameter is substantially constant for said customer's device relative to said previously determined delta of time parameter indicating a low likelihood that said online transaction is fraudulent.

23.   (New) The method of Claim 19 wherein said measured delta of time parameter is compared to said previously determined delta of time parameter to determine whether they fall within a substantially constant range corresponding to said customer's device.

24.   (New) The method of Claim 19 wherein at least one of said measured delta of time parameter and previously determined delta of time parameter is stored by said web server for comparison with a future delta of time parameter measured in the context of a future online transaction to indicate potential fraud.